Reconocimiento de una organización

Organización elegida: *Adobe*

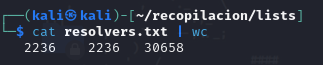
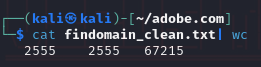
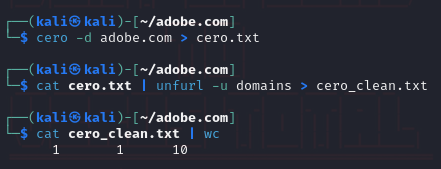
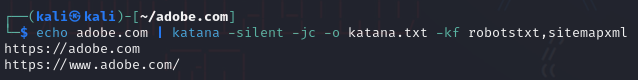
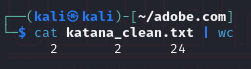
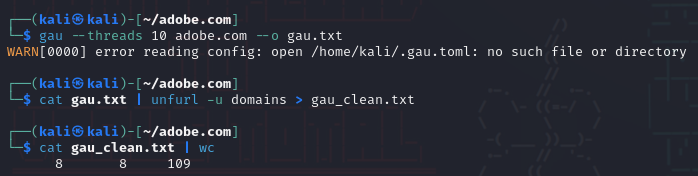
## **Introducción**

🡪 La organización que he seleccionado es Adobe, ya que pertenece al sector de Tecnologías de la Información (TI) y ofrece una extensa variedad de programas y aplicaciones de edición. Al proporcionar servicios en la nube y diversos productos en línea, considero que es una elección idónea para llevar a cabo un análisis y reconocimiento, generando así distintos resultados.

Dominio: \*Adobe.com

🡪Para el reconocimiento de Adobe usaré la distro de Kali Linux junto a numerosas herramientas que nos facilitarán el reconocimiento. El output de todas las herramientas será procesado con Unfurl para extraer el dominio de la URL y dejar un archivo limpio para procesarlo posteriormente sin problema.

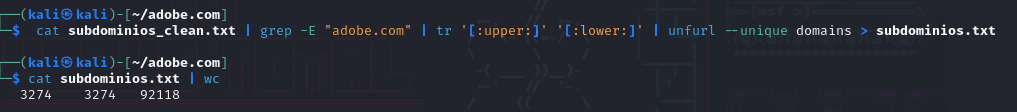
## **Footprinting**

1. Comenzamos creando un fichero con una lista de ips validando que estos servidores DNS sean legítimos y funcionen correctamente (resolvers.txt)
   * 
2. Nos descargamos de un repositorio SecLists un diccionario con posibles dominios (domains.txt)
3. Usamos la herramienta shuffledns para descubrir subdominios asociados a nuestro dominio (adobe.com) objetivo.
   * 
   * 
   * 
4. Comprobamos si utiliza nuestro objetivo Google Analytics:
   *  En este caso Adobe no lo utiliza
5. Otra herramienta que he utilizado es Findomain para seguir encontrando subdominios
   * 
   * 
   * 
6. A continuación, pasaremos Assetfinder para añadir aún más subdominios a nuestra lista:
   * 
7. En numerosas ocasiones el certificado ssl/tls contiene subdominios así que utilizaremos una herramienta para añadir subdominios a nuestra gran lista:
   * 
   * En esta ocasión no hemos encontrado ningún subdominio de interés
8. Seguimos con una herramienta de web scraping para obtener información de forma recursiva y extraer todo el contenido de una web, en este caso: Katana
   * En el comando que lanzo a continuación lanzo Katana sobre los ficheros robots.txt y sitemap.xml los cuales están en la gran mayoría de las webs de las corporaciones.
   * 
   * 
   * 
9. Otra forma de buscar subdominios es utilizar los logs de certificados de transparencia para proporcionar información en tiempo real de los certificados emitidos para un determinado dominio. En este caso utilizaremos la herramienta CTFR
   * 
10. Como ultima herramienta (y no por ello menos importante) utilizaremos Gau, la cual busca a través de varios servicios de la web del dominio elegido varios dominios que se encuentran y se encontraban en antigua versiones de la web.
    * 

🡪Unificamos todos los ficheros de los outputs que nos han devuelto las herramientas en uno solo llamado subdominios\_clean.txt



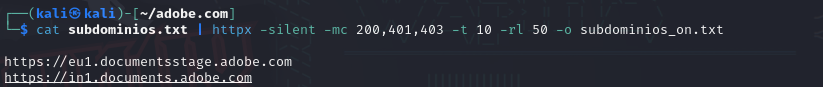
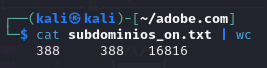
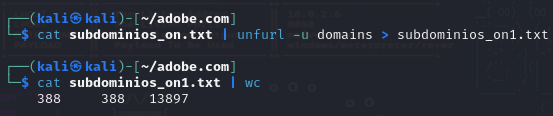
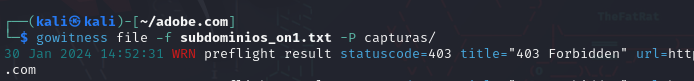
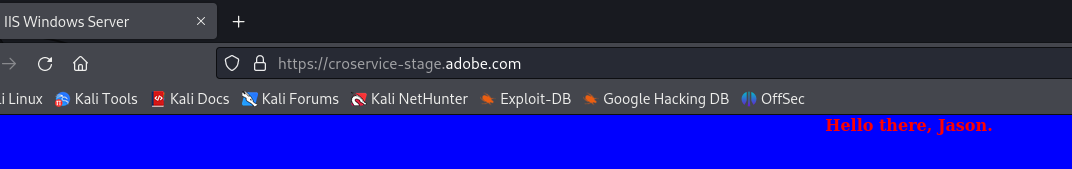
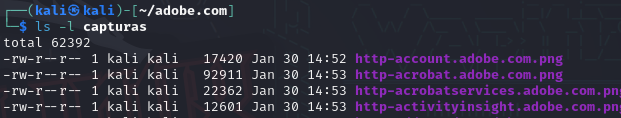
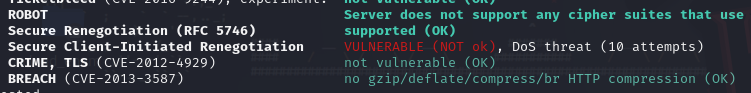
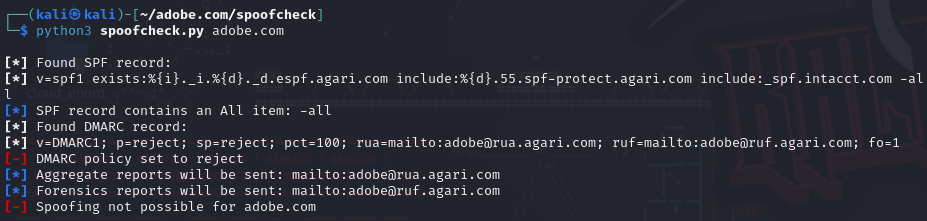
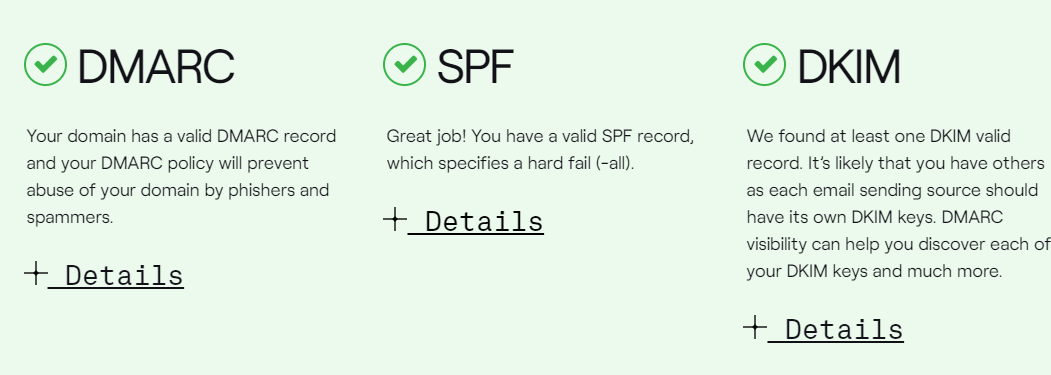
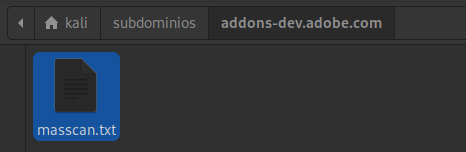
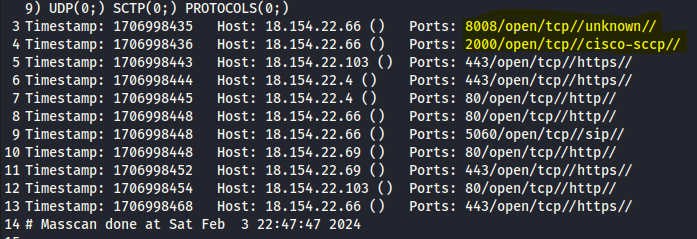




🡪Aun limpiando el fichero nos quedamos con bastantes subdominios.

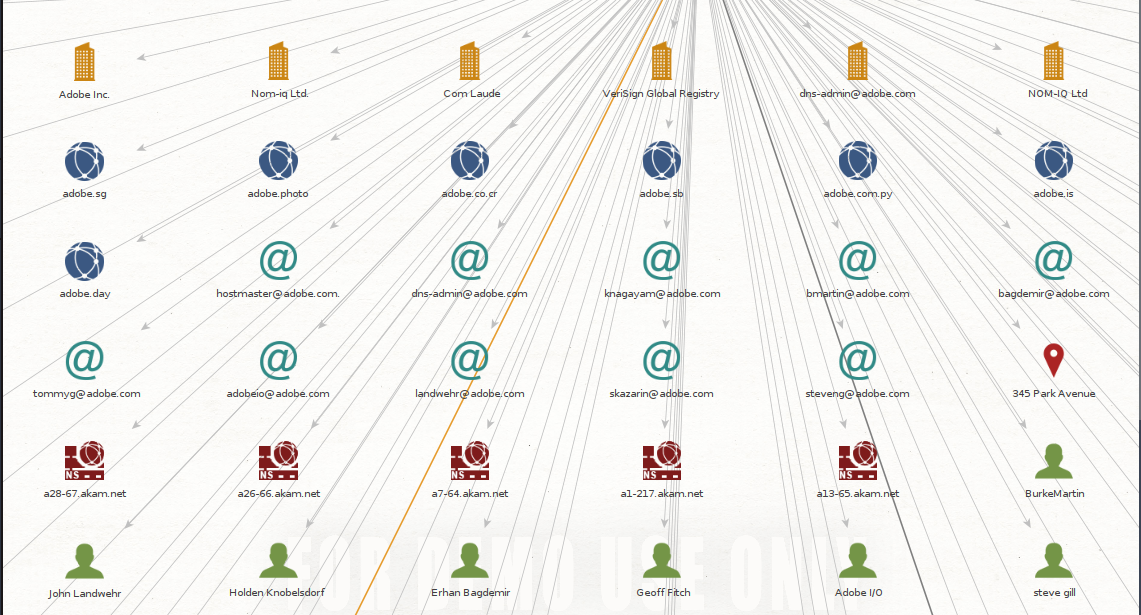
## **Fingerprinting**

🡪Ahora que ya hemos hecho una búsqueda exhaustiva de subdominios procedemos a trabajar con ellos.

1. Antes de analizar los dominios en busca de puertos y demás información haremos una criba de subdominios para quedarnos solo con los activos: En este caso contamos con la herramienta HTTPX que nos facilita el trabajo:
   1. 
   2. 
   3. 
2. Una captura de los subdominios sería de gran ayuda para saber de un vistazo que es lo que alberga cada uno, en esta ocasión utilizaré Gowitness:
   1. 
   2. Las capturas las almacenaré en una carpeta llamada “capturas”
   3. 
      1. Encontramos cosas curiosas como la presencia de Red-Hat en una de las páginas de adobe
   4. 
      1. También un IIS de Windows server
      2. 
   5. 
3. Analizando la configuración ssl de adobe nos encontramos con más de una vulnerabilidad (o posible vulnerabilidad ya que puede tratarse de un falso positivo) (gracias a la herramienta testssl)
   1. 
   2. 
4. Analizando los servidores de correo también podemos encontrar vulnerabilidades, comprobando los registros DNS con spoofcheck damos un problema con la política DMARC:
   1. 
5. En cambio otra herramienta web no indica ningún problema: 
6. Analizamos a continuación que puertos están abiertos en las ips de los subdominios que hemos recopilado utilizando la herramienta masscan
   1. 
   2. 
   3. En el subdominio addons-dev.adobe.com hemos encontrado que se encuentran 2 puertos abiertos fuera de la común: 3003 y 2000. El 8008 no nos ofrece mucha información mientras que el 2000 nos indica que estamos ante un protocolo de telefonía IP Cisco en concreto un Skinny Client Control Protocol.

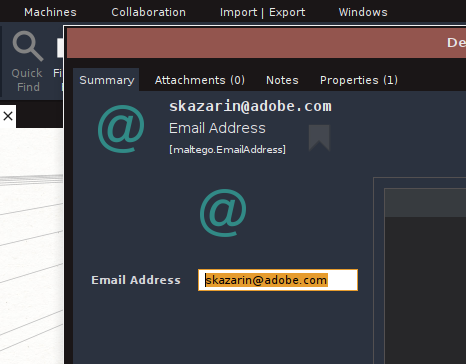
## **OSINT**

MALTEGO

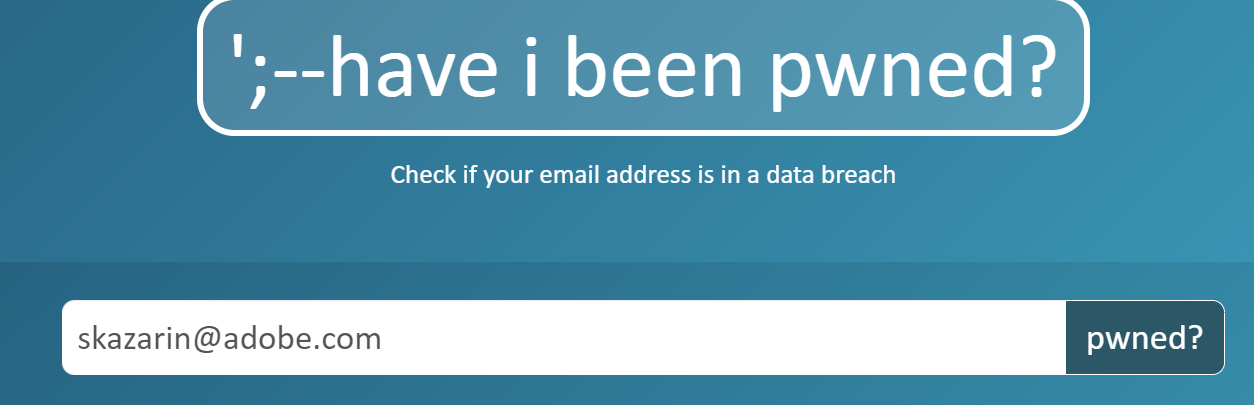


-A través de maltego podemos indagar sobre toda clase de información expuesta por Adobe en la red. Vamos a escoger un par de casos para realizar el OSINT.

-En primer caso escogemos el correo electrónico: [skazarin@adobe.com](mailto:skazarin@adobe.com)

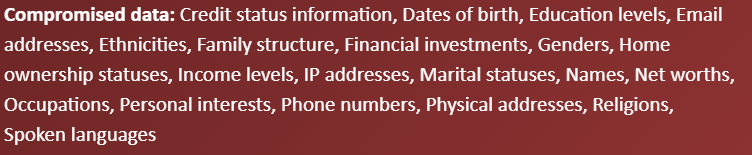


Existen páginas web como por ejemplo <https://haveibeenpwned.com/> que nos permiten saber si se ha filtrado y donde se ha filtrado un correo electrónico.

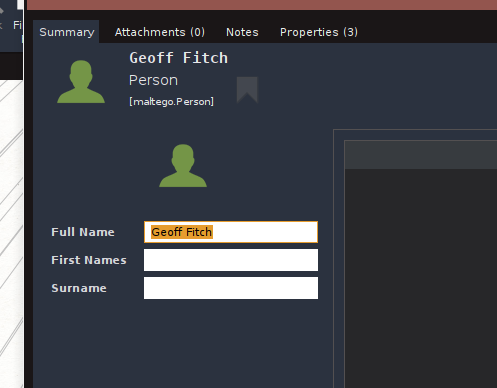
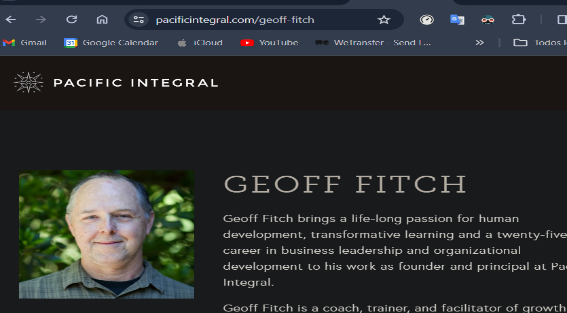


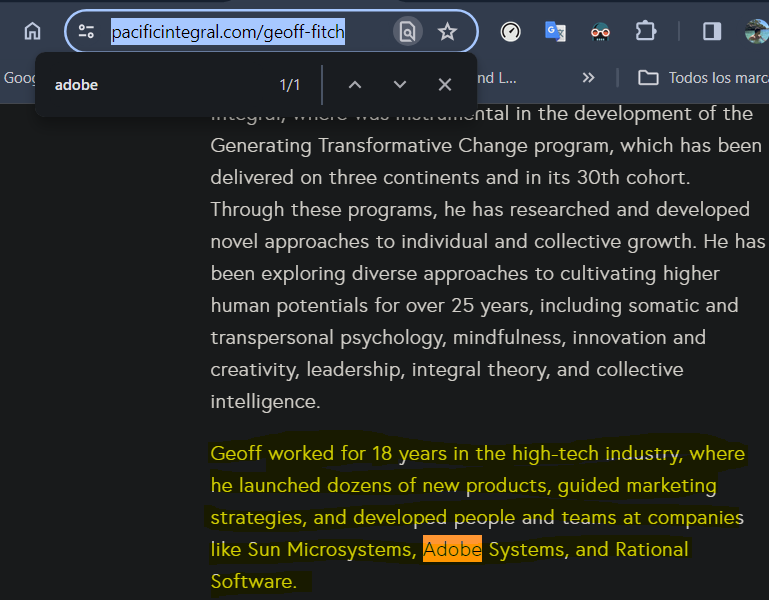


Este correo elecronico por ejemplo se ha filtrado a través de 8 fuentes distintas:

* Apollo
* Data & Leads
* Data Enrichment Exposure From PDL Customer
* Exactis
  + A través de exactis se filtró una gran cantidad de información delicada:
  + 
* LinkedIn
* NetProspex
* Verifications.io
* You've Been Scraped

Como segundo caso elegiremos el nombre de una persona: Geoff Fitch

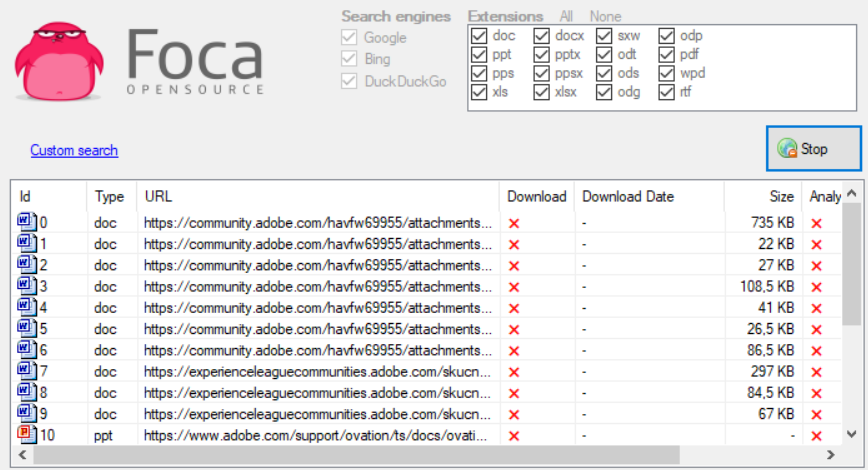




Con una simple búsqueda en internet podemos recabar toda la información de una persona.

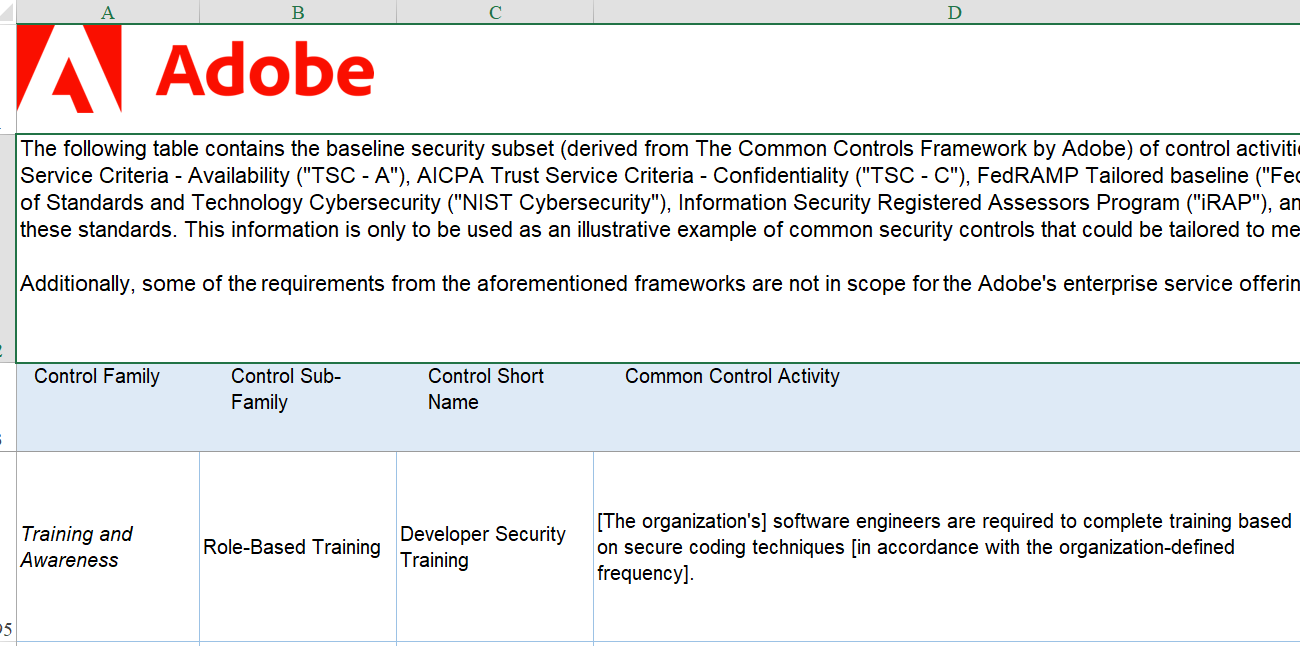


FOCA



Un ejemplo de archivos encontrados con Foca, es un archivo .xlsx (Una tabla excel) que nos muestra el subconjunto de seguridad básico (derivado del Marco de controles comunes de Adobe) de las actividades de control que se aplican a las ofertas de servicios empresariales de Adobe.

🡪Las actividades de control ayudan a que las ofertas empresariales de Adobe cumplan con los requisitos de ISO/IEC 27001, ISO 22301, Criterios de servicio de confianza AICPA - Criterios comunes (TSC - CC), Criterios de servicio de confianza AICPA - Disponibilidad ("TSC - A"), Criterios de servicio de confianza AICPA … Y demás criterios que están obligados a cumplir.



## **Conclusión Final o Resumen:**

1. **Footprinting:**
   * Se llevó a cabo un proceso exhaustivo de footprinting utilizando diversas herramientas en el entorno de Kali Linux.
   * La búsqueda de subdominios se realizó mediante herramientas como Shuffledns, Findomain, Assetfinder, CTFR, y Gau.
   * El análisis de la estructura web incluyó la utilización de Katana para obtener información recursiva y examinar archivos como robots.txt y sitemap.xml.
   * Se generó un archivo consolidado llamado "subdominios\_clean.txt" que contenía todos los subdominios identificados.
2. **Fingerprinting:**
   * Los subdominios identificados fueron sometidos a una criba utilizando la herramienta HTTPX para filtrar los subdominios activos.
   * Gowitness se utilizó para capturar imágenes de las páginas web asociadas a los subdominios, revelando información interesante, como la presencia de Red Hat e IIS en ciertas páginas de Adobe.
   * Se identificaron posibles vulnerabilidades en la configuración SSL mediante la herramienta Testssl y se examinaron los servidores de correo en busca de problemas, detectándose un problema con la política DMARC.
   * Masscan se utilizó para analizar los puertos abiertos en las IPs de los subdominios, revelando información sobre el protocolo de telefonía IP Cisco en un caso específico.
3. **OSINT (Open Source Intelligence):**
   * Maltego se empleó para realizar OSINT sobre la organización Adobe, con énfasis en la búsqueda de información relacionada con un correo electrónico específico (skazarin@adobe.com) y el nombre de una persona (Geoff Fitch).
   * La información recopilada reveló filtraciones de correo electrónico en múltiples fuentes y proporcionó detalles sobre actividades de control de seguridad aplicadas a las ofertas empresariales de Adobe.
   * Se utilizó FOCA para buscar información en archivos expuestos en la red, revelando un archivo .xlsx que detallaba el subconjunto de seguridad básico aplicado a las ofertas empresariales de Adobe.